UNCLASSIFIED

McAfee VirusScan Locally Configured Client

Version: 4

Release: 2

23 April 2010

STIG.DOD.MIL

Sort Order: Group ID (Vulid), ascending order
Notice: Developed by DISA for the DoD
Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System= SECRET Checklist
Top Secret System = SECRET Checklist

Group ID (Vulid): V-6453
Group Title: DTAM001-McAfee VirusScan Control Panel
Rule ID: SV-6538r5_rule
Severity: CAT I
Rule Version (STIG-ID): DTAM001
Rule Title: The McAfee VirusScan Control Panel parameters are not configured as required.

Vulnerability Discussion: This parameter controls if the scan is started at startup.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration

Criteria: If the value of bStartDisabled is 0, this is not a finding. If the value is 1, this is a finding

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On access scanner\McShield\Configuration

Criteria: If the value of bStartDisabled is 0, this is not a finding. If the value is 1, this is a finding

Fix Text: Change the value of registry key HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration so that the value of bStartDisabled is 0.

Fix Text: Change the value of registry key HKLM\Software\McAfee\VSCore\OnAccess
Scanner\McShield\configuration so that the value of bStartDisabled is 0.

Group ID (Vulid): V-6467
Group Title: DTAM002-McAfee VirusScan on access scan boot sect
Rule ID: SV-6554r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM002
Rule Title: The McAfee VirusScan on access scan parameter for Boot sectors is incorrect.

Vulnerability Discussion: This parameter controls if boot sectors are scanned at startup.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration

Criteria: If the value of bDontScanBootSectors is 0, this is not a finding. If the value is 1, this is a finding

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\Mcshield\configuration

Criteria: If the value of bDontScanBootSectors is 0, this is not a finding. If the value is 1, this is a finding

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration so that the value of bDontScanBootSectors is 0.
Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\OnAccess Scanner\McShield\Configuration so that the value of bDontScanBootSectors is 0.

Group ID (Vulid): V-6468
Group Title: DTAM003-McAfee VirusScan on access scan floppy
Rule ID: SV-6555r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM003
Rule Title: The McAfee VirusScan on access scan parameter for floppy disks is incorrect.

Vulnerability Discussion: This parameter controls the scanning of floppy disks.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration

Criteria: If the value of bScanFloppyonShutdown is 1, this is not a finding. If the value is 0, this is a finding

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McfAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of bScanFloppyonShutdown is 1, this is not a finding. If the value is 0, this is a finding

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration so that the value of bScanFloppyonShutdown is 1.
Fix Text: Change the registry key HKLM\SoftwareMcAfee\VSCore\
On Access Scanner\mcshield\Configuration so that the value of bScanFloppyonShutdown is 1.

Group ID (Vulid): V-6469
Group Title: DTAM004-McAfee VirusScan message dialog

Rule ID: SV-6556r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM004
Rule Title: The McAfee VirusScan message dialog parameters are not configured as required.

Vulnerability Discussion: This parameter notifies the user when a virus is detected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_AutoShowList is 1, this is not a finding. If the value is 0, this is a finding

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On access scanner\Mcshield\Configuration

Criteria: If the value of Alert_AutoShowList is 1, this is not a finding. If the value is 0, this is a finding

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration so that the value of Alert_AutoShowList is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of Alert_AutoShowList is 1.

Group ID (Vulid): V-6470
Group Title: DTAM005-McAfee VirusScan remove messages
Rule ID: SV-6557r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM005
Rule Title: The McAfee VirusScan remove messages parameters are not configured as required.

Vulnerability Discussion: This parameter controls if users can remove virus alerts from the display.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanRemove is 0, this is not a finding. If the value is 1, this is a finding

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanRemove is 0, this is not a finding. If the value is 1, this is a finding

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration so that the value of Alert_UsersCanRemove is 0.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\
On Access Scanner\mcshield\Configuration so that the value of Alert_UsersCanRemove is 0.

Group ID (Vulid): V-6471
Group Title: DTAM006-McAfee VirusScan Clean Infected file
Rule ID: SV-6558r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM006
Rule Title: The McAfee VirusScan Clean Infected file parameter is not configured as required.

Vulnerability Discussion: This parameter deteremines if infected files are cleaned.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanClean is 1, this is not a finding. If the value is 0, this is a finding

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Mcafee\VSCore\
On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanClean is 1, this is not a finding. If the value is 0, this is a finding

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\mcshield\Configuration so that the value of Alert_UsersCanClean is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\
On Access Scanner\mcshield\Configuration so that the value of Alert_UsersCanClean is 1.

Group ID (Vulid): V-6472
Group Title: DTAM007-McAfee VirusScan delete infected file
Rule ID: SV-6559r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM007
Rule Title: The McAfee VirusScan delete infected file parameter is not configured as required.

Vulnerability Discussion: This parameter controls if infected files are deleted.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanDelete is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanDelete is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration so that the value of Alert_UsersCanDelete is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of Alert_UsersCanDelete is 1.

Group ID (Vulid): V-6473
Group Title: DTAM008-McAfee VirusScan quarantine parameter
Rule ID: SV-6560r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM008
Rule Title: The McAfee VirusScan quarantine parameter is not configured as required.

Vulnerability Discussion: This parameter controls if infected files are moved to a quarantine folder.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanQuarantine is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of Alert_UsersCanQuarantine is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration so that the value of Alert_UsersCanQuarantine to 1.
Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of Alert_UsersCanQuarantine to 1.

Group ID (Vulid): V-6474
Group Title: DTAM009-McAfee VirusScan Control Panel log
Rule ID: SV-6561r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM009
Rule Title: The McAfee VirusScan Control Panel log parameter is not configured as required.

Vulnerability Discussion: This parameter controls the logging of the scan.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLogtoFile is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLogtoFile is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration so that the value of bLogtoFile is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of bLogtoFile is 1.

Group ID (Vulid): V-6475
Group Title: DTAM010-McAfee VirusScan limit log size parameter
Rule ID: SV-6562r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM010
Rule Title: The McAfee VirusScan limit log size parameter is not configured as required.

Vulnerability Discussion: This parameter controls the log size.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLimitSize is 1, and the dwMaxLogSizeMB is at least Hex 64 or bLimitSize is 0 this is not a finding. If the bLimitSize is 0 and dwMaxLogSizeMB is less than Hex 64, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

bLimitSize=1 and dwMaxLogSizeMB=x64 (100)

Criteria: If the value of bLimitSize is 1, and the dwMaxLogSizeMB is at least x64 (100)

or bLimitSize is 0 this is not a finding.

If the bLimitSize is 1 and dwMaxLogSizeMB is less than x64 (100), this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access

Scanner\mcshield\Configuration so that the value of bLimitSize is 1, and the value of dwMaxLogSizeMB is equal to or greater than Hex 64 or bLimitSize is 0.
Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of bLimitSize = 1, and the value of dwMaxLogSizeMB is equal to or greater than x64 (100) (limit size to a max of x64)

or bLimitSize is 0. (do not limit size)

Group ID (Vulid): V-6476
Group Title: DTAM011-McAfee VirusScan log session parameter
Rule ID: SV-6563r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM011
Rule Title: The McAfee VirusScan log session parameter is not configured as required.

Vulnerability Discussion: This parameter controls if session settings are being logged.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLogSettings is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLogSettings is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration so that the value of bLogSettings is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of bLogSettings is 1.

Group ID (Vulid): V-6478
Group Title: DTAM012-McAfee VirusScan log summary parameter
Rule ID: SV-6565r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM012
Rule Title: The McAfee VirusScan log summary parameter is not configured as required.

Vulnerability Discussion: This parameter controls if the session summary is being logged.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLogSummary is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLogSummary is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of bLogSummary is 1.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value of bLogSummary is 1, this is not a finding. If the value is 0, this is a finding.

Group ID (Vulid): V-6583
Group Title: DTAM013-McAfee VirusScan log encrypted files param
Rule ID: SV-6693r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM013
Rule Title: The McAfee VirusScan log encrypted files parameter is not configured as required.

Vulnerability Discussion: This parameter controls if failure to scan encrypted files is logged.

Responsibility: System Administrator

Check Content:
Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value ReportEncryptedFiles is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value ReportEncryptedFiles is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of ReportEncryptedFiles is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration so that the value of ReportEncryptedFiles is 1.

Group ID (Vulid): V-6584
Group Title: DTAM014-McAfee VirusScan log user name parameter

Rule ID: SV-6694r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM014
Rule Title: The McAfee VirusScan log user name parameter is not configured as required.

Vulnerability Discussion: This parameter controls if the user name is logged.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration

Criteria: If the value bLogUserName is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration

Criteria: If the value bLogUserName is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\On Access Scanner\mcshield\Configuration so that the value of bLogUserName is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\mcshield\Configuration so that the value of bLogUserName is 1.

Group ID (Vulid): V-6585
Group Title: DTAM016-McAfee VirusScan autoupdate parameters
Rule ID: SV-6695r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM016
Rule Title: The McAfee VirusScan autoupdate parameters are not configured as required.

Vulnerability Discussion: This parameter ensure that the product is configured to get autoupdates.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\McAfee\DesktopProtection\Tasks\{A14CD6FC-3BA8-4703-87BF-e3247CE382F5}
Criteria:
If bSchedEnabled=1 and eScheduleType=0 the schedule is daily, this is not a finding.
If bSchedEnabled=1 and eScheduleType=1 the schedule is weekly, this is not a finding.
If bSchedEnabled=0, no schedule is set, then this is afinding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{A14CD6FC-3BA8-4703-87BF-e3247CE382F5}
Criteria:
If bSchedEnabled=1 and eScheduleType=0, the schedule is daily, this is not a finding.
If bSchedEnabled=1 and eScheduleType=1, the schedule is weekly, this is not a finding.
If bSchedEnabled=0, no schedule is set, then this is a finding.

Fix Text: On the VirusScan console, Double click the AutoUpdate item, click the Schedule button. On the TASK tab, check the Enable box, and enable the schedule. On the Schedule tab, create a DAILY or WEEKLY schedule to run.
Fix Text: Use the Task | On-Access Scan PropertiesAutoupdate Dialog, set the autoupdates to update at least weekly.

Group ID (Vulid): V-6586
Group Title: DTAM021-McAfee VirusScan Exchange scanner
Rule ID: SV-6696r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM021
Rule Title: The McAfee VirusScan Exchange scanner is not enabled.

Vulnerability Discussion: This parameter controls if the email client scanner is active.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\GeneralOptions

Criteria: If the value bEnabled is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\GeneralOptions

Criteria: If the value bEnabled is 1, this is not a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\GeneralOptions so that the value of bEnabled is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\GeneralOptions so that the value of bEnabled is 1.

Group ID (Vulid): V-6587
Group Title: DTAM022-McAfee VirusScan find unknown programs
Rule ID: SV-6697r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM022
Rule Title: The McAfee VirusScan find unknown programs email parameter is not configured as required.

Vulnerability Discussion: This parameter controls if scanning is performed for unknown program viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value dwProgramHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions

Criteria: If the value dwProgramHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions so that the value of dwProgramHeuristicsLevel is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions so that the value of dwProgramHeuristicsLevel is 1.

Group ID (Vulid): V-6588
Group Title: DTAM023- McAfee VirusScan find unknown macro virus
Rule ID: SV-6698r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM023
Rule Title: The McAfee VirusScan find unknown macro virus email parameter is not configured as required.

Vulnerability Discussion: This parameter controls the scanning for unknown macro viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\EMail scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value dwMacroHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions

Criteria: If the value dwMacroHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\EMail Scanner\Outlook\OnDelivery\DetectionOptions so that the value of dwMacroHeuristicsLevel is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions so that the value of dwMacroHeuristicsLevel is 1.

Group ID (Vulid): V-6589
Group Title: DTAM026-McAfee VirusScan scan inside archives emai
Rule ID: SV-6699r5_rule

Severity: CAT II
Rule Version (STIG-ID): DTAM026
Rule Title: The McAfee VirusScan scan inside archives email parameter is not configured as required.

Vulnerability Discussion: This parameter controls if the contents of archives are checked for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\EMail scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value ScanArchives is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions

Criteria: If the value ScanArchives is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\eMail Scanner\Outlook\OnDelivery\DetectionOptions so that the value of ScanArchives is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions so that the value of ScanArchives is 1.

Group ID (Vulid): V-6590
Group Title: DTAM027-McAfee VirusScan decode MIME email
Rule ID: SV-6700r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM027
Rule Title: The McAfee VirusScan decode MIME email parameter is not configured as required.

Vulnerability Discussion: This parameter controls if encoded files should be decoded for virus scans.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value ScanMime is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions

Criteria: If the value ScanMime is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\EMail Scanner\Outlook\OnDelivery\DetectionOptions so that the value of ScanMime is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions so that the value of ScanMime is 1.

Group ID (Vulid): V-6591
Group Title: DTAM028-McAfee VirusScan scan e-mail message body
Rule ID: SV-6702r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM028
Rule Title: The McAfee VirusScan scan e-mail message body email parameter is not configured as required.

Vulnerability Discussion: This parameter ensures the email message contents is scanned for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email scanner\outlook\onDelivery\DetectionOptions

Criteria: If the value ScanMessageBodies is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions

Criteria: If the value ScanMessageBodies is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions so that the value of ScanMessageBodies is 1.
Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\DetectionOptions so that the value of ScanMessageBodies is 1.

Group ID (Vulid): V-6592
Group Title: DTAM029-McAfee VirusScan allowed actions email
Rule ID: SV-6704r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM029
Rule Title: The McAfee VirusScan allowed actions email parameter is not configured as required.

Vulnerability Discussion: This parameter controls what actions should happen when a virus is detected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ActionOptions

Criteria: If the value uAction is 2, this is not a finding. If the value is other than 2, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\ActionOptions

Criteria: If the value uAction is 2, this is not a finding. If the value is other than 2, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email scanner\Outlook\Ondelivery\ActionOptions so that the value of uAction is 2.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\ActionOptions so that the value of uAction is 2.

Group ID (Vulid): V-6593
Group Title: DTAM030-McAfee VirusScan action prompt email
Rule ID: SV-6706r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM030
Rule Title: The McAfee VirusScan action prompt email parameter is not configured as required.

Vulnerability Discussion: This parameter ensures appropriate actions are prompted for when a virus is found.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email scanner\Outlook\OnDelivery\ActionOptions

Criteria: If the value dwPromptButton is x1F (31), this is not a finding. If the value is not x1F (31), this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\ActionOptions

Criteria: If the value dwPromptButton is x1F (31), this is not a finding. If the value is not x1F (31), this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email scanner\Outlook\OnDelivery\ActionOptions so that the value of dwPromptButton is x1F (31).

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\ActionOptions so that the value of dwPromptButton is x1F (31).

Group ID (Vulid): V-6594
Group Title: DTAM033-McAfee VirusScan return reply email
Rule ID: SV-6707r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM033
Rule Title: The McAfee VirusScan return reply email parameter is not configured as required.

Vulnerability Discussion: This parameter controls if an email is sent back to the original email sender indicating there was a virus detected.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\AlertOptions

Criteria: If the value bDisplayMessage is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\AlertOptions

Criteria: If the value bDisplayMessage is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\Ondelivery\AlertOptions so that the value of bDisplayMessage is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\AlertOptions so that the value of bDisplayMessage is 1.

Group ID (Vulid): V-6595
Group Title: DTAM034- McAfee VirusScan prompt message email
Rule ID: SV-6708r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM034
Rule Title: The McAfee VirusScan prompt message email parameter is not configured as required.

Vulnerability Discussion: This parameter ensures an appropriate message is displayed for the user to indicate a virus was found within an email.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\AlertOptions --

Criteria: If the value szCustomMessage contains an appropriate alert message, this is not a finding. If the value is blank or does not convey an alert, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\Vshield\E-Mail Scan\AlertOptions --

Criteria: If the value szCustomMessage contains an appropriate alert message, this is not a finding. If the value is blank or does not convey an alert, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email

Scanner\Outlook\Ondelivery\AlertOptions so that the value of szCustomMessage contains an appropriate alert message.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\AlertOptions so that the value of szCustomMessage contains an appropriate alert message

---

Group ID (Vulid): V-6596
Group Title: DTAM035-McAfee VirusScan log to file email
Rule ID: SV-6713r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM035
Rule Title: The McAfee VirusScan log to file email parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that virus scanning sessions for email are logged.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ReportOptions --

Criteria: If the value bLogToFile is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\Vshield\E-Mail Scan\ReportOptions

Criteria: If the value bLogToFile is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ReportOptions so that the value of bLogToFile is 1.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\ReportOptions so that the value of bLogToFile is 1.

Group ID (Vulid): V-6597
Group Title: DTAM036-McAfee VirusScan limit log size email
Rule ID: SV-6715r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM036
Rule Title: The McAfee VirusScan limit log size email parameter is not configured as required.

Vulnerability Discussion: This parameter deteremines the size of the log file to ensure data is available for review.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ReportOptions --

Criteria: If the value of bLimitSize is 1, and the dwMaxLogSizeMB is at least Hex 64 (100) or bLimitSize is 0 this is not a finding. If the bLimitSize is 0 or if dwMaxLogSizeMB is less than Hex 64, (100) this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\Vshield\E-Mail Scan\ReportOptions --

Criteria: If the value of bLimitSize is 1, and the dwMaxLogSizeMB is at least Hex 64 or bLimitSize is 0 this is not a finding. If the bLimitSize is 0 or if dwMaxLogSizeMB is less than Hex 64, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ReportOptions so that the value of bLimitSize is 1 and dwMaxLogSizeMB is at least Hex64 OR bLimitSize is 0.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\ReportOptions so that the value of bLimitSize is 1 and dwMaxLogSizeMB is at least Hex64 OR bLimitSize is 0.

Group ID (Vulid): V-6598
Group Title: DTAM037-McAfee VirusScan log content email
Rule ID: SV-6716r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM037
Rule Title: The McAfee VirusScan log content email parameter is not configured as required.

Vulnerability Discussion: This setting controls the entries that are stored in the virus scanning log.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ReportOptions. --

Criteria: If the value dwLogEvent is x130 (304), this is not a finding. If the value is not x130 (304), this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\Vshield\E-Mail Scan\ReportOptions. --

Criteria: If the value dwLogEvent is 1b0, this is not a finding. If the value is not 1b0, this is a finding.

Fix Text: Change the registry key HKLM\Software\McAfee\VSCore\Email Scanner\OnDelivery\ReportOptions so that the value of dwLogEvent is x130 (304).

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\vshield\E-Mail Scan\ReportOptions so that the value of dwLogEvent is 1b0.

Group ID (Vulid): V-6599
Group Title: DTAM045-McAfee VirusScan fixed disk and processes
Rule ID: SV-6717r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM045
Rule Title: The McAfee VirusScan fixed disk and running processes are not configured as required.

Vulnerability Discussion: This parameter ensures that all fixed disks and running processes are scanned for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}
Criteria: For the values of szScanItemx (where x>=0), an entry for Fixed Drives and Special memory must exist. For example, if the following entries exist, this is not a finding.

szScanItem0: FixedDrives
szScanItem1: SpecialMemory

The entries can be in any order and assigned to any number as long as the number is less than the value of UscanNumItems.

If either of these entries are not present or the number of szScanItem is > UscanNumItems, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}
Criteria: For the values of szScanItemx (where x>=0), an entry for Fixed Drives and Special memory must exist. For example, if the following entries exist, this is not a finding.

szScanItem0: FixedDrives
szScanItem1: SpecialMemory

The entries can be in any order and assigned to any number as long as the number is less than the value of UscanNumItems.

If either of these entries are not present or the number of szScanItem is > UscanNumItems, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that entries exist for Fixed Drives and Special Memory. For example, szScanItem0: FixedDrives and szScanItem1: SpecialMemory. The entries can be in any order and assigned to any number as long as the number is less than the value of UscanNumItems.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that entries exist for Fixed Drives and Special Memory. For example, szScanItem0: FixedDrives and szScanItem1: SpecialMemory. The entries can be in any order and assigned to any number as long as the number is less than the value of UscanNumItems.

Group ID (Vulid): V-6600
Group Title: DTAM046-McAfee VirusScan include subfolders
Rule ID: SV-6718r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM046
Rule Title: The McAfee VirusScan include subfolders parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that subfolders are scanned for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bScanSubDirs is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value bScanSubDirs is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bScanSubDirs is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of bScanSubDirs is 1.

Group ID (Vulid): V-6601
Group Title: DTAM047-McAfee VirusScan include boot sectors
Rule ID: SV-6719r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM047
Rule Title: The McAfee VirusScan include boot sectors parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that the boot sector is scanned for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bSkipBootScan is 0, this is not a finding. If the value is 1, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value bSkipBootScan is 0, this is not a finding. If the value is 1, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bSkipBootScan is 0.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of bSkipBootScan is 0.

Group ID (Vulid): V-6602
Group Title: DTAM048-McAfee VirusScan scan all files parameter
Rule ID: SV-6720r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM048
Rule Title: The McAfee VirusScan scan all files parameter is not configured as required.

Vulnerability Discussion: This parameter ensures all files are scanned.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bScanAllFiles is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}
Criteria: If the value bScanAllFiles is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so the value of bScanAllFiles is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so the value of bScanAllFiles is 1.

Group ID (Vulid): V-6604
Group Title: DTAM050-McAfee VirusScan exclusions parameter
Rule ID: SV-6723r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM050
Rule Title: The McAfee VirusScan exclusions parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that there are no exclusions from the virus scanning.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\
CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value NumExcludeItems =0, this is not a finding. If the value is > 0 this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value NumExcludeItems =0, this is not a finding. If the value is > 0 this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of NumExcludeItems is 0.
Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of NumExcludeItems is 0.

Group ID (Vulid): V-6611
Group Title: DTAM052-McAfee VirusScan scan archives parameter
Rule ID: SV-6731r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM052
Rule Title: The McAfee VirusScan scan archives parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that archive files are checked for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value ScanArchives is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}
Criteria: If the value ScanArchives is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of ScanArchives is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of ScanArchives is 1.

Group ID (Vulid): V-6612
Group Title: DTAM053-McAfee VirusScan decode MIME encoded
Rule ID: SV-6732r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM053
Rule Title: The McAfee VirusScan decode MIME encoded files parameter is not configured as required.

Vulnerability Discussion: This file ensures that MIME encoded files are scanned for viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value ScanMime is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value ScanMime is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of ScanMime is 1.
Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of ScanMime is 1.

Group ID (Vulid): V-6614
Group Title: DTAM054-McAfee VirusScan find unknown programs
Rule ID: SV-6734r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM054
Rule Title: The McAfee VirusScan find unknown programs parameter is not configured as required.

Vulnerability Discussion: This parameter will ensure the virus scanner checks for unknown program viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value dwProgramHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}
Criteria: If the value dwProgramHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of dwProgramHeuristicsLevel is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of dwProgramHeuristicsLevel is 1.

Group ID (Vulid): V-6615
Group Title: DTAM055-McAfee VirusScan find unknown macro virus
Rule ID: SV-6735r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM055
Rule Title: The McAfee VirusScan find unknown macro viruses parameter is not configured as required.

Vulnerability Discussion: This parameter controls checking for unknown macro viruses.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value dwMacroHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}
Criteria: If the value dwMacroHeuristicsLevel is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of dwMacroHeuristicsLevel is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of dwMacroHeuristicsLevel is 1.

Group ID (Vulid): V-6616
Group Title: DTAM056-McAfee VirusScan action for Virus
Rule ID: SV-6736r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM056
Rule Title: The McAfee VirusScan action for Virus parameter is not configured as required.

Vulnerability Discussion: This parameter controls the action when a virus is found.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value uAction is 5, this is not a finding. If the value is other than 5, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value uAction is 5, this is not a finding. If the value is other than 5, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of uAction is 5.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of uAction is 5.

Group ID (Vulid): V-6617
Group Title: DTAM057-McAfee VirusScan secondary action
Rule ID: SV-6737r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM057
Rule Title: The McAfee VirusScan secondary action for virus parameter is not configured as required.

Vulnerability Discussion: This parameter controls the secondary action that is performed when a virus is found.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value uSecAction is 3, this is not a finding. If the value is other than 3, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}
Criteria: If the value uSecAction is 2, this is not a finding. If the value is other than 2, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of uSecAction is 3.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of uSecAction is 2.

Group ID (Vulid): V-6618
Group Title: DTAM059-McAfee VirusScan log to file parameter
Rule ID: SV-6738r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM059
Rule Title: The McAfee VirusScan log to file parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that virus scan activities are written to a log file.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bLogToFile is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}
Criteria: If the value bLogToFile is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bLogToFile is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of bLogToFile is 1.

Group ID (Vulid): V-6620
Group Title: DTAM060-McAfee VirusScan log file limit parameter
Rule ID: SV-6740r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM060
Rule Title: The McAfee VirusScan log file limit parameter is not configured as required.

Vulnerability Discussion: This parameter determines the minimum size for the log to ensure enough data is available for review.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value of bLimitSize is 1, and the uKilobytes is at least 19000 or bLimitSize is 0 this is not a finding. If the bLimitSize is 0 and uKilobytes is less than 19000, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value of bLimitSize is 1, and the uKilobytes is at least x5000 (20480) or bLimitSize is 0 this is not a finding. If the bLimitSize is 0 or if uKilobytes is less than x5000(20480), this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bLimitSize is 1 and uKilobytes is >= 19000 OR bLimitSize is 0.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of bLimitSize is 1 and uKilobytes is >= x5000 (20480) OR bLimitSize is 0.

Group ID (Vulid): V-6621
Group Title: DTAM061-McAfee VirusScan log session settings
Rule ID: SV-6741r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM061
Rule Title: The McAfee VirusScan log session settings parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that session settings are logged.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bLogSettings is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value bLogSettings is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bLogSettings is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of bLogSettings is 1.

Group ID (Vulid): V-6624
Group Title: DTAM062-McAfee VirusScan log session summary
Rule ID: SV-6744r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM062
Rule Title: The McAfee VirusScan log session summary parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that session summary information is logged for future review if needed.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bLogSummary is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value bLogSummary is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bLogSummary is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of bLogSummary is 1.

Group ID (Vulid): V-6625
Group Title: DTAM063-McAfee VirusScan failure on encrypted file
Rule ID: SV-6745r7_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM063
Rule Title: The McAfee VirusScan failure on encrypted files parameter is not configured as required.

Vulnerability Discussion: This parameter ensures that failures on encrypted files are logged.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bLogScanEncryptFail is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value bLogScanEncryptFail is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bLogScanEncryptFail is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of bLogScanEncryptFail is 1.

Group ID (Vulid): V-6626

Group Title: DTAM064-McAfee VirusScan log user name
Rule ID: SV-6746r6_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM064
Rule Title: The McAfee VirusScan log user name is not configured as required.

Vulnerability Discussion: This parameter controls the user name being logged as part of the log file.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bLogUserName is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2}

Criteria: If the value bLogUserName is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bLogUserName is 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7
F6C4D2} so that the value of bLogUserName is 1.

Group ID (Vulid): V-6627
Group Title: DTAM070-McAfee VirusScan schedule
Rule ID: SV-6747r8_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM070
Rule Title: The McAfee VirusScan schedule is not configured as required.

Vulnerability Discussion: This parameter ensures that the virus scan is scheduled to be executed.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value bSchedEnabled is 1 and eScheduletype is 0 or 1, this is not a finding.

If the value bSchedEnabled is 0 or eScheduletype is not 0 or not 1 this is a finding.

Check Content:

Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7-F6C4D2}

Criteria: If the value bSchedEnabled is 1 and eScheduletype is 0 or 1, this is not a finding.

If the value bSchedEnabled is 0 or eScheduletype is not 0 or not 1 this is a finding.

Fix Text: Change the registry key HKLM\Software\Network Associates\TVD\VirusScan Enterprise\CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS} so that the value of bSchedEnabled is 1 and eScheduletype is 0 or 1.

Fix Text: Change the registry key HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7-F6C4D2} so that the value of bSchedEnabled is 1 and eScheduletype is 0 or 1.

Group ID (Vulid): V-14618
Group Title: DTAM090-McAfee VirusScan onaccess scan scripts
Rule ID: SV-15243r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM090
Rule Title: The McAfee VirusScan on access scan parameter for scipt scan is incorrect.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\ScriptScan

Criteria: If the value of ScriptScanEnabled is 1, this is not a finding.

This finding applies to Version 8.0 only.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\Script Scanner
Criteria: If the value of ScriptScanEnabled is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\ScriptScan

Criteria: Set the value of ScriptScanEnabled to 1.

This finding applies to Version 8.0 only.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\SoftwareMcAfee\VSCore\Script Scanner

Criteria: Set the value of ScriptScanEnabled to 1.

Group ID (Vulid): V-14619
Group Title: DTAM091-McAfee VirusScan onaccess scan blocking
Rule ID: SV-15244r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM091
Rule Title: The McAfee VirusScan on access scan parameter for connection blocking is incorrect.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlock is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlock is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: Set the value of VSIDBlock to 1.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: Set the value of VSIDBlock to 1.

Group ID (Vulid): V-14620
Group Title: DTAM092-McAfee VirusScan onaccess scan blocking
Rule ID: SV-15245r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM092
Rule Title: The McAfee VirusScan on access scan parameter for connection blocking time is incorrect.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlockTimeout >= to HEX 1E, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlockTimeout >= to HEX 1E, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: Set the value of VSIDBlockTimeout >= to HEX 1E.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: Set the value of VSIDBlockTimeout >= to HEX 1E.

Group ID (Vulid): V-14621
Group Title: DTAM093-McAfee VirusScan onaccess scan blocking
Rule ID: SV-15246r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM093
Rule Title: The McAfee VirusScan on access scan parameter for blocking unwanted programs is incorrect.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlockOnNonVirus is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value of VSIDBlockOnNonVirus is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: Set the value of VSIDBlockOnNonVirus to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: Set the value of VSIDBlockOnNonVirus to 1.

Group ID (Vulid): V-14622
Group Title: DTAM100-McAfee VirusScan scan default values

Rule ID: SV-15247r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM100
Rule Title: The McAfee VirusScan scan default values for processes are not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration

Criteria: If the value OnlyUseDefaultConfig is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration
Criteria: If the value OnlyUseDefaultConfig is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration

Criteria: Set the value OnlyUseDefaultConfig to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration

Criteria: Set the value OnlyUseDefaultConfig to 1.

Group ID (Vulid): V-14623
Group Title: DTAM101-McAfee VirusScan scan when writing disk
Rule ID: SV-15248r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM101
Rule Title: The McAfee VirusScan scan when writing to disk is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: If the value bScanIncoming is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value bScanIncoming is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value bScanIncoming to 1.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value bScanIncoming to 1.

Group ID (Vulid): V-14624
Group Title: DTAM102-McAfee VirusScan scan when reading
Rule ID: SV-15249r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM102
Rule Title: The McAfee VirusScan scan when reading parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: If the value bScanOutgoing is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value bScanOutgoing is 1, this is not a finding

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value bScanOutgoing to 1.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value bScanOutgoing to 1.

Group ID (Vulid): V-14625
Group Title: DTAM103-McAfee VirusScan scan all files parameter
Rule ID: SV-15250r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM103
Rule Title: The McAfee VirusScan scan all files parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: If the value LocalExtensionMode is 1 and the value of NetworkExtensionMode is 1 this is not a finding. If either of these is not 1, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value LocalExtensionMode is 1 and the value of NetworkExtensionMode is 1 this is not a finding. If either of these is not 1, this is a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value LocalExtensionMode to 1and the value of NetworkExtensionMode to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value LocalExtensionMode to 1 and the value of NetworkExtensionMode to 1.

Group ID (Vulid): V-14626
Group Title: DTAM104-McAfee VirusScan heuristics program
Rule ID: SV-15251r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM104
Rule Title: The McAfee VirusScan heuristics program viruses parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: If the value dwProgramHeuristicsLevel is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value dwProgramHeuristicsLevel is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value dwProgramHeuristicsLevel to 1.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value dwProgramHeuristicsLevel to 1.

Group ID (Vulid): V-14627
Group Title: DTAM105-McAfee VirusScan heuristics macro level
Rule ID: SV-15252r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM105
Rule Title: The McAfee VirusScan heuristics macro viruses parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: If the value dwMacroHeuristicsLevel is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value dwMacroHeuristicsLevel is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value dwMacroHeuristicsLevel to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value dwMacroHeuristicsLevel to 1.

Group ID (Vulid): V-14628
Group Title: DTAM106-McAfee VirusScan scan inside archive
Rule ID: SV-15253r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM106
Rule Title: The McAfee VirusScan scan inside archives parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: Information Assurance Officer

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access

Scanner\McShield\Configuration\Default

Criteria: If the value ScanArchives is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value ScanArchives is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value ScanArchives to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value ScanArchives to 1.

Group ID (Vulid): V-14629
Group Title: DTAM107-McAfee VirusScan scan MIME files parameter
Rule ID: SV-15254r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM107
Rule Title: The McAfee VirusScan scan MIME files parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: If the value ScanMime is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value ScanMime is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value ScanMime to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value ScanMime to 1.

Group ID (Vulid): V-14630
Group Title: DTAM110-McAfee VirusScan process primary action
Rule ID: SV-15255r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM110
Rule Title: The McAfee VirusScan process primary action parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: If the value UAction_Program is 1, 3, 4, or 5, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value UAction_Program is 1, 3, 4, or 5, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value UAction_Program to 1, 3, 4, or 5.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value UAction_Program to 1, 3, 4, or 5.

Group ID (Vulid): V-14631
Group Title: DTAM111-McAfee VirusScan process secondary action
Rule ID: SV-15256r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM111
Rule Title: The McAfee VirusScan process secondary action parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: If the value USecAction_Program is 1, 3, 4, or 5, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: If the value USecAction_Program is 1, 3, 4, or 5, this is not a finding. If the value is 0, this is a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration\Default

Criteria: Set the value USecAction_Program to 1, 3, 4, or 5.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\McShield\Configuration\default

Criteria: Set the value USecAction_Program to 1, 3, 4, or 5.

Group ID (Vulid): V-14633
Group Title: DTAM112-McAfee VirusScan log user name parameter
Rule ID: SV-15258r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM112
Rule Title: The McAfee VirusScan log user name parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration

Criteria: If the value bLogUserName is 1, this is not a finding. If the value is 0, this is a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\McAfee\VSCORE\On Access Scanner\McShield\Configuration

Criteria: If the value bLogUserName is 1, this is not a finding. If the value is 0, this is a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\McShield\Configuration

Criteria: Set the value bLogUserName to 1.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\VSCORE\On Access Scanner\McShield\Configuration

Criteria: Set the value bLogUserName to 1.

Group ID (Vulid): V-14651
Group Title: DTAM038-McAfee VirusScan detect unwanted program
Rule ID: SV-15277r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM038
Rule Title: he McAfee VirusScan detects unwanted programs email parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\Vshield\E-Mail Scan\DetectionOptions

Criteria: If the value ApplyNVP is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions

Criteria: If the value ApplyNVP is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\Vshield\E-Mail Scan\DetectionOptions

Criteria: Set the value ApplyNVP to 1.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\DetectionOptions

Criteria: Set the value ApplyNVP to 1.

Group ID (Vulid): V-14652
Group Title: DTAM039-McAfee VirusScan unwanted programs action
Rule ID: SV-15278r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM039
Rule Title: The McAfee VirusScan unwanted programs action email parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\Vshield\E-Mail Scan\ActionOptions

Criteria: If the value uAction is 2, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ActionOptions

Criteria: If the value uAction is 2, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\Vshield\E-Mail Scan\ActionOptions

Criteria: Set the value uAction to 2.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\Email Scanner\Outlook\OnDelivery\ActionOptions

Criteria: Set the value uAction to 2.

Group ID (Vulid): V-14654
Group Title: DTAM058-McAfee VirusScan check unwanted programs
Rule ID: SV-15280r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM058
Rule Title: The McAfee VirusScan check for unwanted programs parameter is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\
CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: If the value ApplyNVP is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\tasks\{21221C11-A06D-4558-B833-98E8C7F6C4D2}

Criteria: If the value ApplyNVP is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\VirusScan Enterprise\
CurrentVersion\Tasks\{818C7543-358A-4C84-899A-14334EMS4BGS}

Criteria: Set the value ApplyNVP to 1.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\McAfee\DesktopProtection\Tasks\{21221C11-A06D-4558-B833-98E8C7F6C4D2}

Criteria: Set the value ApplyNVP to 1.

Group ID (Vulid): V-14657
Group Title: DTAM130-McAfee VirusScan buffer overflow protectio
Rule ID: SV-15283r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM130
Rule Title: The McAfee VirusScan buffer overflow protection is not configured as required.

Vulnerability Discussion: This setting is required for the virus software.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\BehaviourBlocking

Criteria: If the value EnterceptEnabled is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\BehaviourBlocking

Criteria: Set the value EnterceptEnabled to 1.

Group ID (Vulid): V-14658
Group Title: DTAM131-McAfee VirusScan buffer overflow protectio
Rule ID: SV-15284r5_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM131
Rule Title: The McAfee VirusScan buffer overflow protection mode is not configured as required.

Vulnerability Discussion: This setting is required to ensure that buffer overflow protection is enabled and that "Protection mode" is enabled. Buffer overflow protection prevents tampered with application code from being executed on the computer. The "Protection mode" option is selected to ensure that the application is prevented from executing.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\BehaviourBlocking

Criteria: If the value EnterceptMode is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\BehaviourBlocking

Criteria: Set the value EnterceptMode to 1.

Group ID (Vulid): V-14659
Group Title: DTAM132-McAfee VirusScan buffer overflow message
Rule ID: SV-15285r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM132
Rule Title: The McAfee VirusScan buffer overflow message parameter is not configured as required.

Vulnerability Discussion: This setting is required to ensure when buffer overflow protection is enabled that the "Show the messages dialog box when a buffer overflow is detected" is selected. Buffer overflow protection prevents tampered with application code from being executed on the computer. The "Show the messages dialog box when a buffer overflow is detected" option is selected to ensure that the user is notified .

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\BehaviourBlocking

Criteria: If the value EnterceptShowMessages is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\
On Access Scanner\BehaviourBlocking

Criteria: Set the value EnterceptShowMessages to 1.

Group ID (Vulid): V-14660
Group Title: DTAM133-McAfee VirusScan buffer overflow log
Rule ID: SV-15286r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM133
Rule Title: The McAfee VirusScan buffer overflow log parameter is not configured as required.

Vulnerability Discussion: This setting is required to ensure when buffer overflow protection is enabled that the "Enable activity logging and accept the default location for the log file or specify a new location" is selected. Buffer overflow protection prevents tampered with application code from being executed on the computer. The "Enable activity logging and accept the default location for the log file or specify a new location" option is selected to ensure that buffer overflow logging is being performed .

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: If the value bLogToFile_Ent is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value bLogToFile_Ent is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: Set the value bLogToFile_Ent to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: Set the value bLogToFile_Ent to 1.

Group ID (Vulid): V-14661

Group Title: DTAM134-McAfee VirusScan log size limitation
Rule ID: SV-15287r4_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM134
Rule Title: The McAfee VirusScan log size limitation parameters are not configured as required.

Vulnerability Discussion: This setting is required to ensure when buffer overflow protection is enabled that the "Log file size" is selected. Buffer overflow protection prevents tampered with application code from being executed on the computer. The "Log file size" option is selected to ensure that buffer overflow log file size does not excced 100mb.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: If the value bLimitSize_Ent is 1 and the value of dwMaxLogSizeMB_Ent is at least hex 64, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: If the value bLimitSize_Ent is 1 and the value of dwMaxLogSizeMB_Ent is at least x40 (64), this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\On Access Scanner\BehaviourBlocking

Criteria: Set the value bLimitSize_Ent to 1and the value of dwMaxLogSizeMB_Ent to at least hex 64.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\On Access Scanner\BehaviourBlocking

Criteria: Set the value bLimitSize_Ent to 1and the value of dwMaxLogSizeMB_Ent to at least x40 (64).

Group ID (Vulid): V-14662
Group Title: DTAM135-McAfee VirusScan detection of Spyware
Rule ID: SV-15288r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM135
Rule Title: The McAfee VirusScan detection of Spyware is not configured as required.

Vulnerability Discussion: This setting is required to ensure that under the Unwanted Programs Policies, Spyware is selected. This enables the detection of Spyware on the system.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\NVP

Criteria: If the value DetectSpyware is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\NVP

Criteria: If the value DetectSpyware is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\NVP

Criteria: Set the value DetectSpyware to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\NVP

Criteria: Set the value DetectSpyware to 1.

Group ID (Vulid): V-14663
Group Title: DTAM136-McAfee VirusScan detection of Adware
Rule ID: SV-15289r3_rule
Severity: CAT II
Rule Version (STIG-ID): DTAM136
Rule Title: The McAfee VirusScan detection of Adware is not configured as required.

Vulnerability Discussion: This setting is required to ensure that under the Unwanted Programs Policies, Adware is selected. This enables the detection of Adware on the system.

Responsibility: System Administrator

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\NVP

Criteria: If the value DetectAdware is 1, this is not a finding.

Check Content:
Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\NVP

Criteria: If the value DetectAdware is 1, this is not a finding.

Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\Software\Network Associates\TVD\Shared Components\NVP

Criteria :Set the value DetectAdware to 1.
Fix Text: Procedure: Use the Windows Registry Editor to navigate to the following key:
HKLM\software\McAfee\VSCore\NVP

Criteria :Set the value DetectAdware to 1.

Group ID (Vulid): V-19910
Group Title: Virus Signature Files older that 7 days.
Rule ID: SV-22081r1_rule

Severity: CAT I
Rule Version (STIG-ID): DTAG008
Rule Title: The antivirus signature file age exceeds 7 days.

Vulnerability Discussion: Antivirus signature files are updated almost daily by antivirus software vendors. These files are made available to antivirus clients as they are published. Keeping virus signature files as current as possible is vital to the security of any system.

Note: If the vendor or trusted site's files match the date of the signature files on the machine, this is not a finding.

Responsibility: System Administrator

Check Content:
Locate McAfee icon in system tray. Right click to open and choose VirusScan Console. Select Help then choose About VirusScan Enterprise. Displayed will be a date for "DAT Created On:.

Criteria: If the "DAT Created On:" date is older than 7 calendar days from the current date, this is a finding.

Note: If the vendor or trusted site's files are also older than 7 days and match the date of the signature files on the machine, this is not a finding.

Fix Text: Update antivirus signature file as your local process describes e.g autoupdate or runtime executable.

UNCLASSIFIED